

Децентрализованные системы

Криптовалюты

Биткоин

ДАО - Децентрализованная Автономная Организация.

Понятней всего рассматривать ДАО как систему, работающую без участия человека, под контролем неизменного набора параметров и правил.

ДАО - Децентрализованная Автономная Организация.

Автономная - не имеет влияния разработчика.

Дистрибутивная - отсутствуют центральные узлы.

Прозрачная - любой может изучить алгоритм.

Конфиденциальная - данные пользователя защищены.

Бездоверительная - нет необходимости слепо доверять системе.

Саморегулируемая - регуляция заложена в алгоритме.

Неподкупная - никто не может повлиять на принцип работы.

Интернет

Проявление “межсетевого слоя” ДАО

Глобальная система взаимосвязанных
компьютерных сетей.

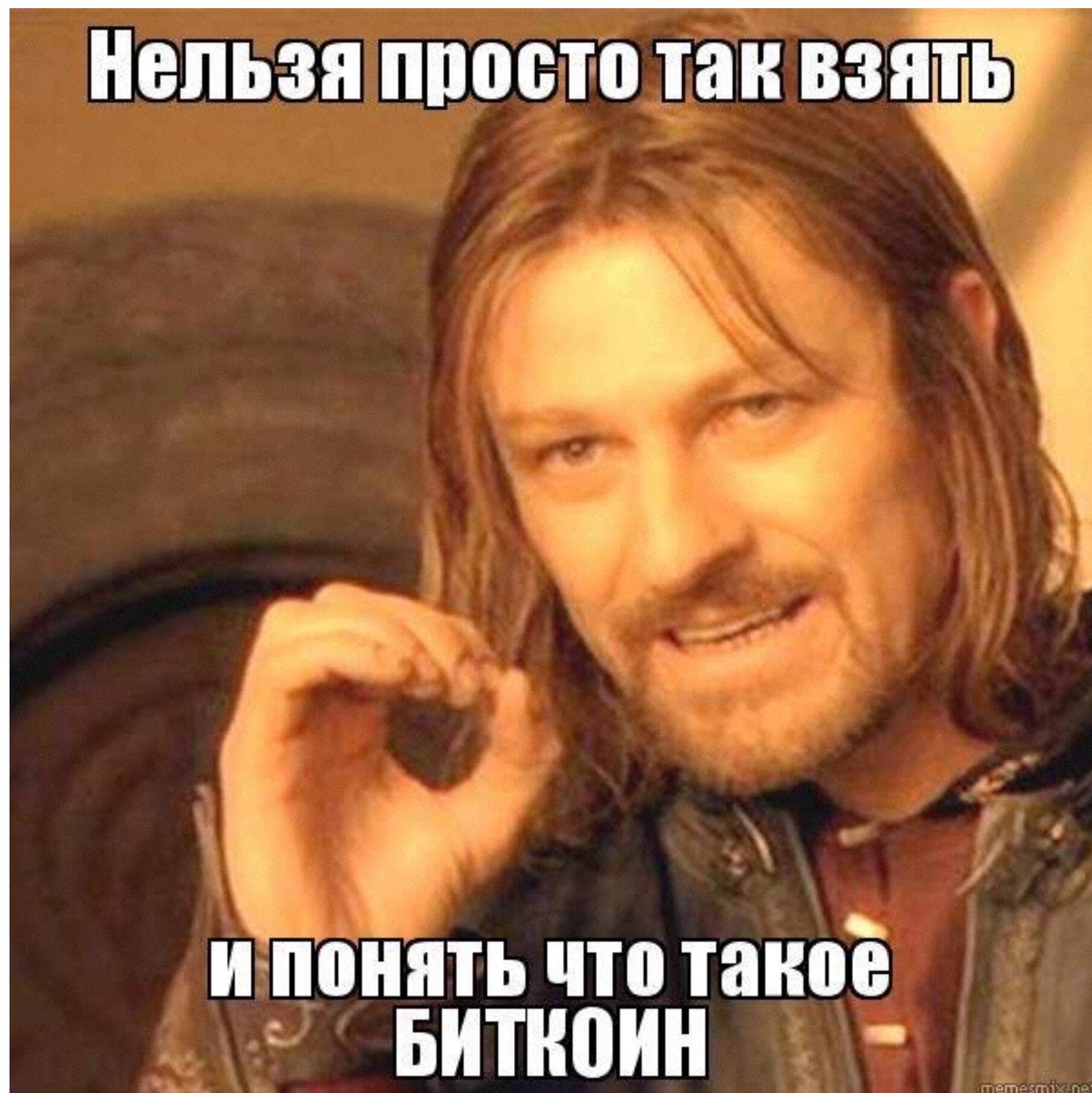
Криптовалюта

Проявление экономического потенциала ДАО

Криптовалюта - технологическое явление; Система взаиморасчетов между людьми без участия третьих лиц.

Систему поддерживают ее же участники. Эмиссия контролируется алгоритмом, а ее цель - стимуляция активности и покрытие затрат людей, участвующих в процессе получения эмиссии.

Биткоин - Первая реализация Криптовалюты



Биткоин - Первая реализация Криптовалюты

Биткоин - криптовалюта.

Биткоин - Первая реализация Криптовалюты

Биткоин

- это платежная система.
- это интернет деньги.
- это электронное золото.
- это виртуальные наличные.
- это способ передачи денег на расстояние.
- это бесплатные международные переводы.
- это анонимные платежи.

*Пусть каждый придумает себе свое толкование.

Биткоин - Первая реализация Криптовалюты

Код Биткоин - открытый репозиторий, в основном, на языке C++.

Блокчейн - база данных с информацией обо всех операциях с 2009 года.

Блок - фрагмент базы данных, содержащий некое количество транзакций.

Транзакция - перевод биткоинов с одного адреса на другой или нескольких адресов на несколько.

Биткоин адрес – единственный способ хранения биткоина.

Приватный ключ - признак принадлежности адреса его владельцу.

Биткоин - Первая реализация Криптовалюты

Приватный ключ - набор символов, генерируемый локально на компьютере. Он известен только Вам. Именно с его помощью Вы сможете отправлять биткоины с соответствующего адреса.

*Подобрать технически невозможно. Для этого понадобится 43(62 знака) лет.
 2^{256} комбинаций.

Биткоин - Первая реализация Криптовалюты

Биткоин адрес - следствие приватного ключа. Используется для создания транзакции, может выступать отправителем и получателем.

Биткоин - Первая реализация Криптовалюты

Транзакция - операция перевода биткоинов между адресами.

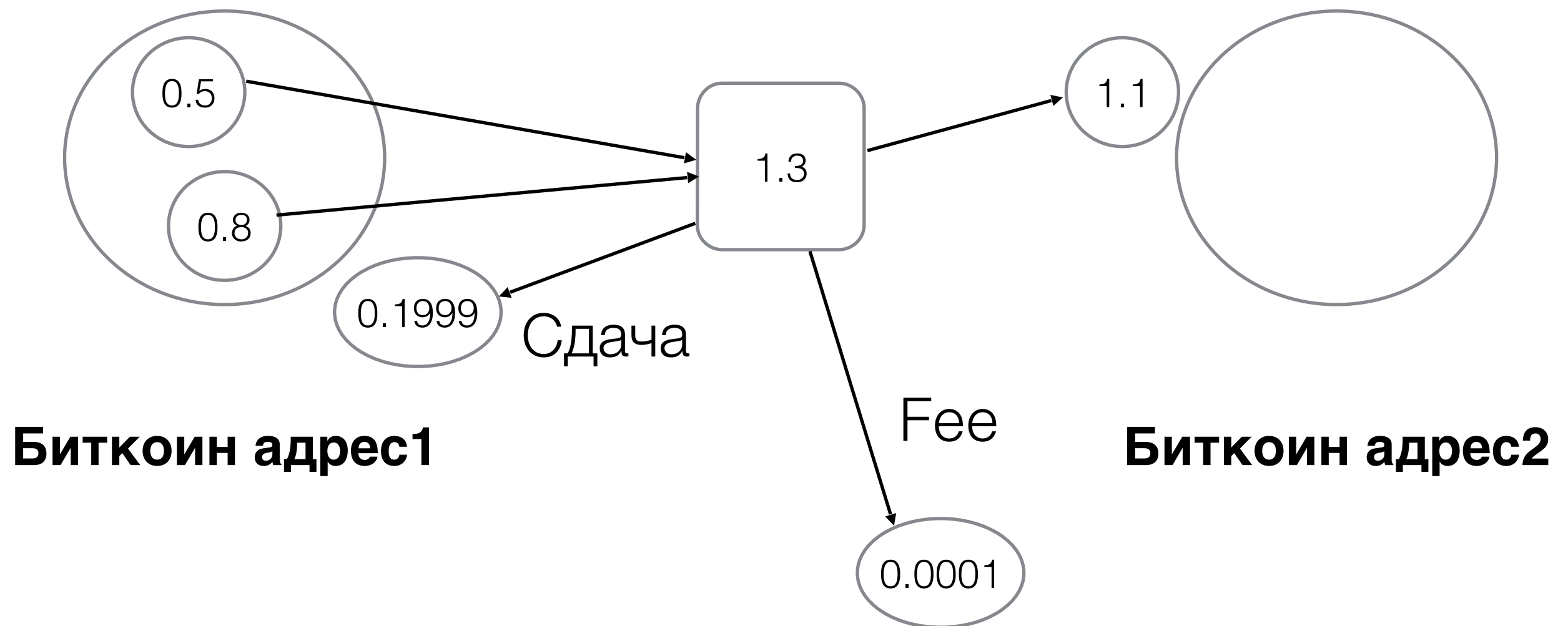
Важно!

Биткоин нельзя приравнивать к счету в банке и перевод нельзя приравнивать к изменению цифры суммы счета.

Пример. Если на ваш адрес была произведена транзакция на сумму 0.5 Биткойна, а потом еще 0.8, это значит, что у вас есть **два непотраченных входа** на 0.5 и 0.8 биткоинов.

Биткоин - Первая реализация Криптовалюты

Вам необходимо отправить 1.1 Биткоина на Адрес2



Таким образом, баланс на адресе – это сумма всех входящих транзакций **минус** сумма всех исходящих.

Биткоин - Первая реализация Криптовалюты

Блок – некое количество транзакций, которое система должна признать валидным. Время на утверждения и, как следствие, количество транзакций в блоке зависят от везения так называемых “майнеров”.

*тут Макс на пальцах объясняет что такое майнинг.

Биткоин - Первая реализация Криптовалюты

Блокчейн - база всех транзакций за всю историю существования биткоин-системы.

На основании записей в блокчейне рассчитывается сумма биткоинов на конкретном адресе.

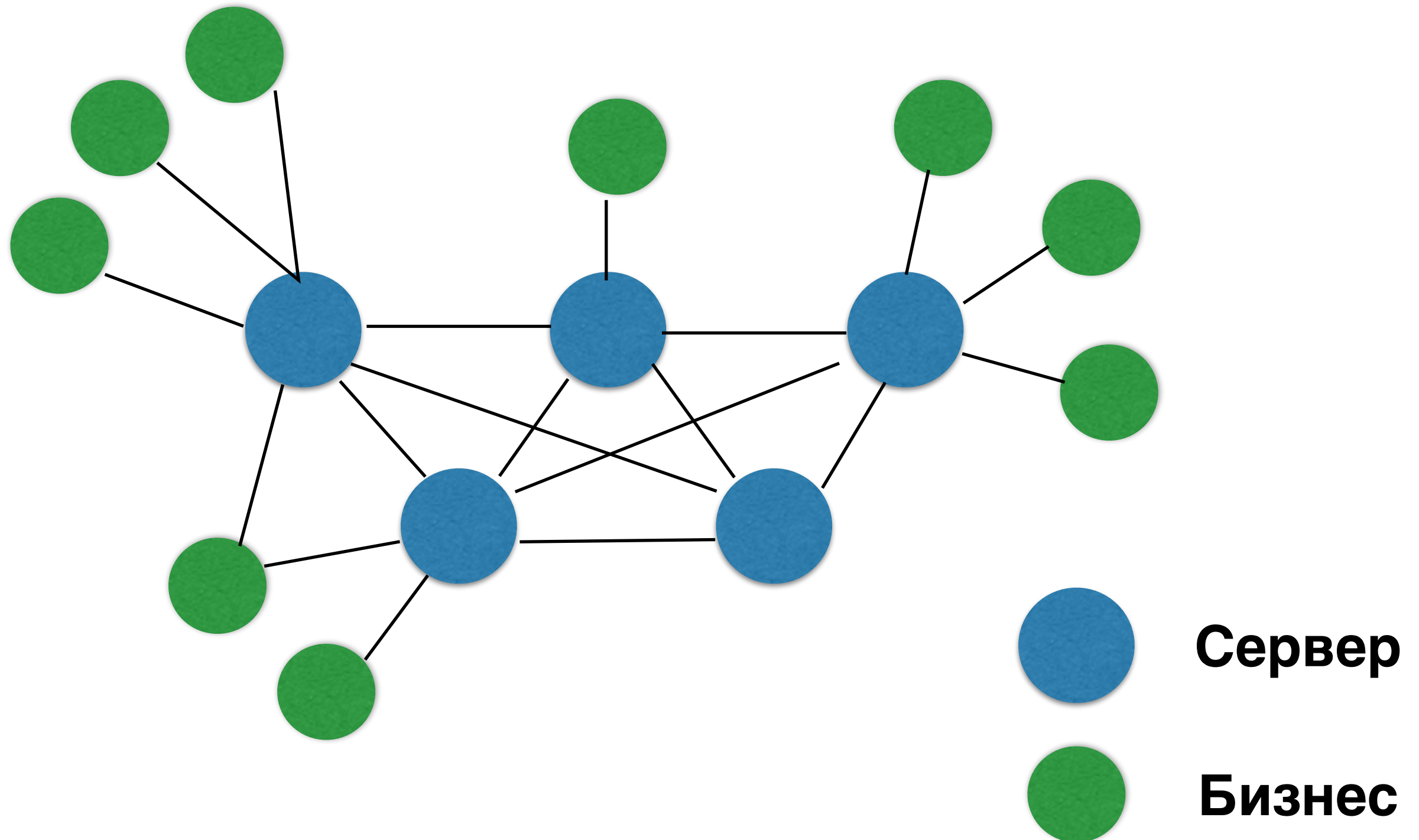
Биткоин - Первая реализация Криптовалюты

Биткоин код - исходный код Биткоин, который запускается с помощью биткоин сервера.

Любой желающий может проверить этот код.
Каждый может запустить этот сервер у себя на компьютере и стать частью сети, приняв принципы ее работы.

Биткоин - Первая реализация Криптовалюты

Биткоин Сеть.



Спасибо

Facebook: Maksym Krupyshev

facebook.com/LogZz.kieff

Bitcoin Foundation Ukraine

facebook.com/groups/bitcoin.ua/